This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-23.   (Cancelled)

24.   (Previously Presented) A method of password generation comprising:

providing a biometric information sample;

determining from the sample a first string including a plurality of symbols, the symbols based on features within the biometric information sample;

determining a plurality of strings in dependence upon predetermined characteristics in relation to the first string;

hashing the strings from the determined plurality of strings to produce a plurality of hash values; and

comparing each hash value from the plurality of hash values against a stored hash value determined during an enrollment process for determining at least one hash string from the plurality of hash strings indicative of a match,

wherein upon a match between a hash value from the plurality of hash values and the stored bash value, the string from the plurality of strings and associated with the matching hash value is provided as die generated password.

25.-27. (Cancelled)

28.   (Original) A method of password generation according to claim 24 wherein the first string is ordered based upon its symbol content.

29.   (Original) A method of password generation according to claim 28 wherein the strings from the plurality of strings are ordered based upon their symbol content.

30.   (Previously Presented) A method of password generation according to claim 24 wherein determining a plurality of strings in dependence upon predetermined characteristics comprises:

capturing an image of a biometric information sample from a biometric information source;

extracting a number r of features from the biometric information sample and encoding r symbols, one per feature; and,

extracting a number δ of extra features, and encoding δ extra symbols, one per extra feature, and

wherein comparing the string includes determining a number of symbols within the

string that are absent from the previously stored string and deleting those symbols.

31.   (Original) A method of password generation according to claim 24 wherein upon the comparison of each hash value from the plurality of hash values against a stored hash value determined during an enrollment process is indicative of other than at least one hash string from the plurality of hash strings matches, verifying if the plurality of hash strings includes all the hash strings that can be generated within predetermined characteristics.

32.   (Original) A method of password generation according to claim 24 wherein the generated password is an unordered generated password.

33.   (Currently Amended) A method of password generation according to claim 24 comprising determining at least a feature type of features within the biometric information sample and encoding symbols from the plurality of symbols in dependence upon the determined at least a feature type.

34.   (Original) A method of password generation according to claim 24 wherein a symbol is encoded as an n-bit value.

35.   (Previously Presented) A method of password generation comprising:

providing a biometric information sample from an individual;

determining a location of an alignment feature within the biometric information sample;

extracting features from the biometric information sample;

determining from the extracted features a first string of symbols based on locations of extracted features within the biometric information sample relative to the alignment feature;

determining a plurality of error strings in dependence upon predetermined parameters defining an error region about the extracted first string;

hashing the first string and at least some of the error strings from the determined plurality of strings to produce a plurality of hash values; and

comparing each produced hash value from the plurality of hash values with a predetermined stored hash value for determining a hash value from the plurality of hash values indicative of a match,

wherein upon a match between a hash value from the plurality of hash values and the stored hash value, the string from which the matching hash value was derived is provided as the generated password.

36.   (Currently Amended) A method of password generation according to claim 35 comprising: providing an indication of the ~~first~~ alignment feature.

37.   (Currently Amended) A method of password generation according to claim 36 wherein providing an indication of the ~~first~~ alignment feature includes selecting the ~~first~~ alignment feature from a plurality of ~~first~~ alignment features.

38.   (Currently Amended) A method of password generation according to claim 36 wherein providing an indication of the ~~first~~ alignment feature includes selecting a region within the biometric information sample, the region being indicative of ~~first~~ alignment feature from a plurality of potential ~~first~~ alignment features.

39.-48. (Cancelled).